AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1 - 21 (Canceled).

Claim 22 (New): A system for maintaining trust in the content of a digital data file, comprising:

a trusted time source to provide a certifiable time for an unalterable time stamp, wherein said certifiable time confirms at least one of said digital data file's access, creation, modification, receipt, or transmission;

a computing means having installed therein a system clock and an operating systems means for operating said computing means;

an application means running on said operating system means, wherein said application means provides an application programming interface (API) between said trusted time source and said application means, and wherein said application programming interface is adapted to select said trusted time source or said system clock in one or more instances, wherein each of said one or more instances corresponds to a request for a determination of a moment in time;

means for receiving said request to save said digital data file from a user;

means for determining said selection of said trusted time source to provide said determination of said moment in time;

first means for saving said digital data file at said moment in time;

means for retrieving from said trusted time source a date and a time corresponding to said moment in time, wherein said moment in time is substantially the current time of said trusted time source corresponding to receipt of said request;

first means for appending said date and said time retrieved from said trusted time source to said digital data file;

first means for signing said digital data file with said date and said time retrieved from said trusted time source appended thereto;

means for hashing said digital data file to produce a digest;

second means for signing said digest with a key to produce a certificate;

second means for appending said certificate to said digital data file;

second means for saving said digital data file with said certificate appended thereto; and

means for verifying trust in the content of said digital data file with said certificate appended thereto.

Claim 23 (New): The system of claim 22, wherein said API prevents said system clock from being accessed when said instance is to be determined by said trusted time source.

Claim 24 (New): The system of claim 22, wherein said one or more instances includes at least one of an operating system call which is unrelated to said application means, an operating system call which is related to said application means, or an application call which is unrelated to said operating system means.

Claim 25 (New): The system of claim 22, wherein said verification means includes a third means for signing said digital data file with said date and said time retrieved from said trusted time source appended thereto with an identifier.

Claim 26 (New): The system of claim 25, wherein said identifier corresponds to said computing means used by said user is elected from the group consisting of a platform identifier, a server node identifier, and a network identifier.

Claim 27 (New): The system of claim 25, wherein said identifier is selected from the group consisting of an identifier corresponding to said user, an identifier corresponding to a system used

by said user, and an identifier corresponding to an enterprise within which said user uses said computing means.

Claim 28 (New): The system of claim 25, wherein said user identifier is selected from the group consisting of a plurality of characters identifying said user, first data representing an iris scan of said user, second data representing a retina scan of said user, third data representing a finger scan of said user, fourth data representing said user's hand geometry, fifth data representing said user's voice, sixth data representing said user's signature, and combinations of said plurality of characters, first, second, third, fourth, fifth, and sixth data.

Claim 29 (New): The system of claim 22, wherein said trusted time source includes a tamper-evident means.

Claim 30 (New): A method for maintaining trust in the content of a digital data file with a computing means having installed therein a system clock, an operating systems means for operating the computing means, and an application means running on said operating system means, comprising:

providing, with a trusted time source, a certifiable time for an unalterable time stamp, wherein said certifiable time confirms at least one of said digital data file's access, creation, modification, receipt, or transmission;

providing an application programming interface (API) between said trusted time source and said application means, and wherein said application programming interface is adapted to select said trusted time source or said system clock in one or more instances, wherein each of said one or more instances corresponds to a request for a determination of a moment in time;

receiving said request to save said digital data file from a user;

determining said selection of said trusted time source to provide said determination of said moment in time;

saving said digital data file at said moment in time;

retrieving from said trusted time source a date and a time corresponding to said moment in time, wherein said moment in time is substantially the current time of said trusted time source corresponding to receipt of said request;

appending said date and said time retrieved from said trusted time source to said digital data file;

signing said digital data file with said date and said time retrieved from said trusted time source appended thereto;

hashing said digital data file to produce a digest;

signing said digest with a key to produce a certificate;

appending said certificate to said digital data file;

saving said digital data file with said certificate appended thereto; and

verifying trust in the content of said digital data file with said certificate appended thereto.

Claim 31 (New): The method of claim 30, wherein said API prevents said system clock from being accessed when said instance is to be determined by said trusted time source.

Claim 32 (New): The method of claim 30, wherein said one or more instances includes at least one of an operating system call which is unrelated to said application means, an operating system call which is related to said application means, or an application call which is unrelated to said operating system means.

Claim 33 (New): The method of claim 30, wherein said verification means includes a third means for signing said digital data file with said date and said time retrieved from said trusted time source appended thereto with an identifier.

Claim 34 (New): The method of claim 33, wherein said identifier corresponds to said computing means used by said user is elected from the group consisting of a platform identifier, a server node identifier, and a network identifier.

Claim 35 (New): The method of claim 33, wherein said identifier is selected from the group consisting of an identifier corresponding to said user, an identifier corresponding to a system used by said user, and an identifier corresponding to an enterprise within which said user uses the computing means.

Claim 36 (New): The method of claim 33, wherein said user identifier is selected from the group consisting of a plurality of characters identifying said user, first data representing an iris scan of said user, second data representing a retina scan of said user, third data representing a finger scan of said user, fourth data representing said user's hand geometry, fifth data representing said user's voice, sixth data representing said user's signature, and combinations of said plurality of characters, first, second, third, fourth, fifth, and sixth data.

Claim 37 (New): The method of claim 30, wherein said trusted time source includes a tamper-evident means.